Europäisches Patentamt

European Patent Office

Office européen des brevets

Bescheinigung

Certificate

Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. Patent application No. Demande de brevet n°

02368128.1

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

R C van Dijk

Anmeldung Nr:
Application no.: 02368128.1
Demande no:

Anmeldetag:
Date of filing: 28.11.02
Date de dépôt:

Anmelder/Applicant(s)/Demandeur(s):

INTERNATIONAL BUSINESS MACHINES CORPORATION

Armonk, NY 10504
ETATS-UNIS D'AMERIQUE

Bezeichnung der Erfindung/Title of the invention/Titre de l'invention:
(Falls die Bezeichnung der Erfindung nicht angegeben ist, siehe Beschreibung.
If no title is shown please refer to the description.
Si aucun titre n'est indiqué se referer à la description.)

Method and system for accessing internet resources through a proxy using the form-based authentication

In Anspruch genommene Prioriät(en) / Priority(ies) claimed /Priorité(s) revendiquée(s)
Staat/Tag/Aktenzeichen/State/Date/File no./Pays/Date/Numéro de dépôt:

Internationale Patentklassifikation/International Patent Classification/
Classification internationale des brevets:

H04L29/06

Am Anmeldetag benannte Vertragstaaten/Contracting states designated at date of filing/Etats contractants désignées lors du dépôt:

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LI LU MC NL PT SE SK TR

METHOD AND SYSTEM FOR ACCESSING INTERNET RESOURCES THROUGH A PROXY USING THE FORM-BASED AUTHENTICATION

Technical field

The present invention relates to the Internet environment wherein a user addresses requests for getting Internet resources to a proxy which transmits these requests to a content server able to provide the Internet resources and relates in particular to a method and system for accessing Internet resources through a proxy using the form-based authentication.

Background

The Service Provider market moves up the value chain from pure connectivity services to deliver value-added and revenue generating services. The business model of a Service Provider which was initially driven by minutes of use is being more and more replaced by data traffic, generated by users that access either internal services owned and maintained by the Service Provider itself or external services not maintained by the Service Provider but accessed through the Service Provider platform. In addition to growing their customer bases, the service providers are now looking to increase the average revenue per user to boost revenues. More compelling services such as content, commerce, and applications promise higher profit margins, improved customer retention, and greater customer satisfaction. Yet, managing and distributing these third-party services or content services present significant challenges to service providers. Therefore, the Service Provider plays a key role since it is the intermediary between the end-user and the internal or external services. Its privileged position allows him to not only provide just "simple" access but added value services such as security, single sign-on, billing, location, etc. at the condition that it cannot be "bypassed" by the user.

In most cases, external services and partners that provide resources will do it for authenticated users only, meaning that they maintain and enforce the authentication and authorization of these users using their own user registry. Therefore, multiple authentication points may exist thus requiring the end-user to maintain multiple user IDs and passwords, and be prompted to authenticate multiple times in order to be able to access his personalized services. Obviously, this represents a fastidious step for the end-user to enter several times a couple of username/password in order to access the Web services and therefore the Service Provider might loose any credibility towards its end-users if it does not provide a solution to this problem. A solution is to provide a "Single Sign On" feature to their end-users giving them the possibility to use the same User Id and password for all services being internal or external that require authentication. With this feature, user authentication only needs to be done once to access services requiring a user Id and password.

At connection time, the Service Provider asks the end-user to identify himself as an authorized user by responding to a username/password prompt displayed on the user device in order to give end-users the benefit of personalized services and resources according to the end-users choices and preferences. As already mentioned, these personalized services and resources can be either internal services managed and maintained by the Service Provider or external services provided by content provider partners.

The Service Providers and service and the content providers partners have to come to an agreement on how passing credentials about the end-users from the Service Provider to the partners. The HTTP protocol is the transport protocol used for each communication involved, in one hand in the exchanges between the device being used to access the internal or external services provided by the service provider which is typically a Web browser and the Service Provider platform, and in other hand between the Service Provider and its service and the partners. Different techniques exist today such as the Basic HTTP Authentication exchange defined in the HTTP standard, the HTTP cookies, customized HTTP headers, … can be used to perform such integration around single sign-on. But this previous cases require business development and cost on each side allowing so the partners to directly trust the authentication done by the Service Provider platform.

The Service Provider being the intermediary between the end-user and the internal or external services and, thanks to its privileged position, uses in most cases an HTTP proxy component deployed in its infrastructure forcing all end-users to go through and acting as a central authentication point for all end-users who wish to access personalized internal and external services and resources.

The two well known and spread authentication methods on Internet are the HTTP Basic Authentication and the Forms-based authentication (a HTML form sent to the end-user prompting him to enter a couple username/password), both over normal or secure encrypted connection. Although performing single sing-on with Basic Authentication is relatively easy (and most of the HTTP proxies in the market already support single sign on to back-end application server representing external service or content provider partners using the HTTP Basic Authentication as described in the HTTP specification) most servers choose not to use it as a means of authentication, primarily because the User Interface is un-sophisticated and set by the Web browser and also because it is limited to a single hostname. Forms-based authentication is much more widely used because it is more flexible. Unfortunately, it is this very flexibility that makes single sign-on to form-based system so much difficult to handle insofar as the forms being used are various and different in function of the servers, thereby requiring a development cost.

Summary of the invention

Accordingly, the main object of the invention is to provide a method and a system allowing the service providers to reduce the cost of development to perform single sing-on in case of partners using a form-based authentication, thereby avoiding any additional development effort and cost on both sides (service providers and partners).

The invention relates therefore to a method for accessing from an Internet user to Internet resources provided by at least a content server in a data transmission system including a proxy connected to the Internet network, the proxy being adapted to perform the form-based authentication of the user when receiving a user request for Internet resources therefrom, and wherein the proxy transmits the user request to the content server which sends back a response to the proxy. Such a method comprises the following steps :

-the transmission from said proxy to a Single Sign On (SSO) Server of the user request together with the credentials associated with the user,

-the filling by the SSO server of a login form obtained from the content server, the form being filled by using the credentials,

-the transmission by the content server to the SSO server of a response to the user request after receiving the filled login form from the SSO server, this response being then sent back to the proxy and,

-the transmission by the proxy of the requested information to the user, the information being contained in the response received by the proxy.

According to another aspect, the invention relates to a data transmission system including a proxy connected to the Internet network and at least a content server to which a user can gain access by the intermediary of the proxy, this one being associated with authentication means adapted to perform the form-based authentication of the user when receiving a user request for Internet resources therefrom and wherein the proxy transmits the user request to the content server which sends back a response to the proxy. The authentication means comprise a Single Sign-On (SSO) server adapted to obtain a login form from the content server when receiving the user request from the proxy, to fill the login form by using the credentials associated with the user and to send back the filled login form thereby playing the role of the user regarding the content server, so that the content server can provide the requested information after authentication of the user.

Brief description of the drawings

The above and other objects, features and advantages of the invention will be better understood by reading the following more particular description of the invention in conjunction with the accompanying drawings wherein :

- Fig. 1 is a schematic block-diagram showing a data transmission system according to the invention.
- Fig. 2 is a schematic block-diagram representing the different data flows achieved between the elements of the data transmission system illustrated in Fig. 1.
- Fig. 3 is a diagram illustrating the flows being achieved for each kind of request being transmitted by the user to

the proxy in the data transmission system illustrated in Fig. 1.

Detailed description of the invention

Referring to Fig. 1 representing a data transmission system used in the context of the invention, a service provider provides Web services to a plurality of users such as user 10 through the Internet network 12. Such web services can be any kind of information which can be furnished by a content server 14. When the user wants to access to the content server, he transmits a request to a proxy 16. This proxy has at its disposal a user registry (not shown) containing the information such as credentials of the users allowed to access the services provided by the service provider (generally the identification and password of the user).

The proxy 16 is connected to a Single Sign-on (SSO) server 18 which is deployed in the service provider platform in order to recognize when a login form is presented and to be able to interpret it and respond accordingly. For this, the SSO server 18 has at its disposal a configuration file 20 which provides details about signing on to the back-end server 14. The role of the configuration file 20 is to specify the URL of the login page into the server 14, the location of the login page, the name of the input field used for "username" and the name of the input field used for "password".

In a preferred embodiment of the invention, the SSO Server 18 is an additional component, external to the proxy 16, and does not assume any specific behaviour different from the standard one that every proxy should implement. But it could also be closely integrated within the proxy itself, thus providing additional advantages (less components, no need for specific service entry point URL) at the additional cost of developing the functionality described in the invention inside it.

The diagram in Fig. 2 illustrates the steps achieved in the method. These steps are the following :

1) The user logs on to the HTTP proxy 16. He accesses the back-end application service in content server 14 by clicking a specific URL provided by the service provider that identifies the service entry point and references to SSO server 18.

2) Upon reception of this request, the HTTP proxy 16 passes the user's authentication information to the SSO server 18 (e.g. A standard HTTP authorization header credential such as the authorization HTTP header described in the HTTP specification).

3) The SSO server 18 generates a GET request using the information from its configuration file, sends it to the content server 14 and obtains the custom login page and any session information such as cookies).

4) The SSO server 18 filters the login form and, using information from its configuration file, fills in the username/password (together with any hidden fields, data, and session cookies).

5) The SSO server 18 generates a POST request and transmits it to the content server 14. This one authenticates the request and returns the result (plus session information if any) back to the SSO server.

6) The SSO server 18 sends the HTTP response and any session information to the HTTP proxy 16.

7) The HTTP proxy 16 forwards this information back to the user 10.

8)-9) All subsequent requests to the content server 14 are routed across the standard junction to the content server (a junction is a configuration rule that exists in the proxy to handle the connection between the proxy and the content server).

The data flows corresponding to the different kinds of requests transmitted from the user are represented in Fig. 3.

A. First request issued by the user

The user sends the first request to the HTTP proxy, invoking the external URL configured in the Proxy (/). Since the invoked URL is protected, the Proxy sends an authentication challenge to the client. Different methods can be used to send this challenge (HTTP response code 401, form,…). This is independent from the authentication technique required by the back-end servers. The user responds with its credentials (typically a user name and password). The Proxy verifies these credentials against its user registry, and accepts them if they correspond to a valid user. It returns a HTTP response to the client.

B. Processing of the HTTP request to the content server

The user now sends a request towards a Back-end Service in the content server. From the invoked URL, the Proxy reroutes this request to the SSO server, augmented by the user credentials (such as the HTTP Authorization Header) collected in step A. The SSO server will then play the role of the user regarding to the content server.

C. Content server authentication procedure

The SSO server invokes the Login Form configured for the content server. This one responds with the Login Form. The SSO server "fill the form", and Post the user credentials to the content server. Since these credentials are valid,the content server sends back an HTTP response to the SSO server, potentially augmented by a session Cookie, specific to the content server. The content of this cookie is opaque to the SSO server and to the Proxy, and will allow the content server to verify, on subsequent requests, that this user has been properly identified. Cookies are important in a form-based login environment because they are often used by the server to identify the users session. Obviously, precautions have to be taken around the Internet domain and the cookies, because a cookie will be replayed by a Web browser if it matches the Internet domain of the HTTP requests submitted. Optionally this response can be combined with a redirection towards the content server, which will allow subsequent requests to flow directly either from the Proxy to the content server, bypassing the SSO Server, or from the user directly to the content server. The SSO server forwards this response back to the Proxy, and then to the user.

D. Subsequent requests

The Proxy forwards subsequent requests directly to the content server, without going through the SSO server. In each request the user repeats the content server Session Cookie (if any), which is used by the content server to retrieve the user context.

CLAIMS

1. Method for accessing from an Internet user (10) to Internet resources provided by at least a content server (14) in a data transmission system including a proxy (16) connected to the Internet network (12), said proxy being adapted to perform the form-based authentication of the user when receiving a user request for Internet resources therefrom, and wherein said proxy transmits the user request to said content server which sends back a response to the proxy;

   said method being characterized in that it comprises the following steps :

   - the transmission from said proxy (16) to a Single Sign On (SSO) Server (18) of said user request together with the credentials associated with said user,
   - the filling by said SSO server of a login form obtained from said content server, said form being filled by using said credentials,
   - the transmission by said content server to said SSO server of a response to said user request after receiving the filled login form from said SSO server, said response being then sent back to said proxy and,
   - the transmission by said proxy of the requested information to said user, said information being contained in said response.

2. Method according to claim 1, wherein said SSO server (18) has at its disposal a configuration file (20) for obtaining and filling said login form, said configuration file providing information about said content server such as the URL of the login page, the location of said login page, the name of the input field used for "username" and the name of the input field used for"password".

3. Method according to claim 2, wherein said response from said content server (14) sent back to said proxy (16) includes at least one cookie specific to said content server.

4. Method according to claim 1, 2 or 3, further comprising an initial step of transmitting by said user (10) a first request to said proxy (16) invoking the external URL configured in said proxy, said proxy sending back an authentication challenge to said user in order to verify the user credentials and checking whether they correspond to a valid user.

5. Method according to claim 4, wherein the subsequent requests after said user request transmitted by said user (10) are forwarded directly from said proxy (16) to said content server (14), the responses containing the requested information being transmitted directly to said proxy by said content server.

6. Data transmission system including a proxy (16) connected to the Internet network (12) and at least a content server (14) to which a user (10) can gain access by the intermediary of said proxy, said proxy being associated with authentication means (18) adapted to perform the form-based authentication of the user when receiving a user request for Internet resources therefrom and wherein said proxy transmits the user request to said content server which sends back a response to said proxy;

said system being characterized in that said authentication means comprise a Single Sign-On (SSO) server adapted to obtain a login form from said content server when receiving said user request from said proxy, to fill said login form by using the credentials associated with said user and to send back the filled login form thereby playing the role of said user regarding said content server, so that said content server can provide the requested information after authentication of said user.

7. Data transmission system according to claim 6, wherein said SSO server (18) has at its disposal a configuration file (20) for obtaining and filling said login form, said configuration file providing information about said content server such as the URL of the login page, the location of said login page, the name of the input field used for "username" and the name of the input field used for"password".

8. Data transmission system according to claim 6 or 7, wherein said SSO server (18) is external to said proxy (16).

9. Data transmission system according to claim 6 or 7, wherein said SSO server (18) is integrated within said proxy

METHOD AND SYSTEM FOR ACCESSING INTERNET RESOURCES THROUGH A PROXY USING THE FORM-BASED AUTHENTICATION

Abstract

Data transmission system including a proxy (16) connected to the Internet network (12) and at least a content server (14) to which a user (10) can gain access by the intermediary of the proxy, the proxy being associated with authentication means (18) adapted to perform the form-based authentication of the user when receiving a user request for Internet resources therefrom and wherein the proxy transmits the user request to the content server which sends back a response to the proxy. The authentication means comprise a Single Sign-On (SSO) server adapted to obtain a login form from the content server when receiving the user request from the proxy, to fill the login form by using the credentials associated with the user and to send back the filled login form thereby playing the role of the user regarding the content server, so that the content server can provide the requested information after authentication of the user.

FIG. 1

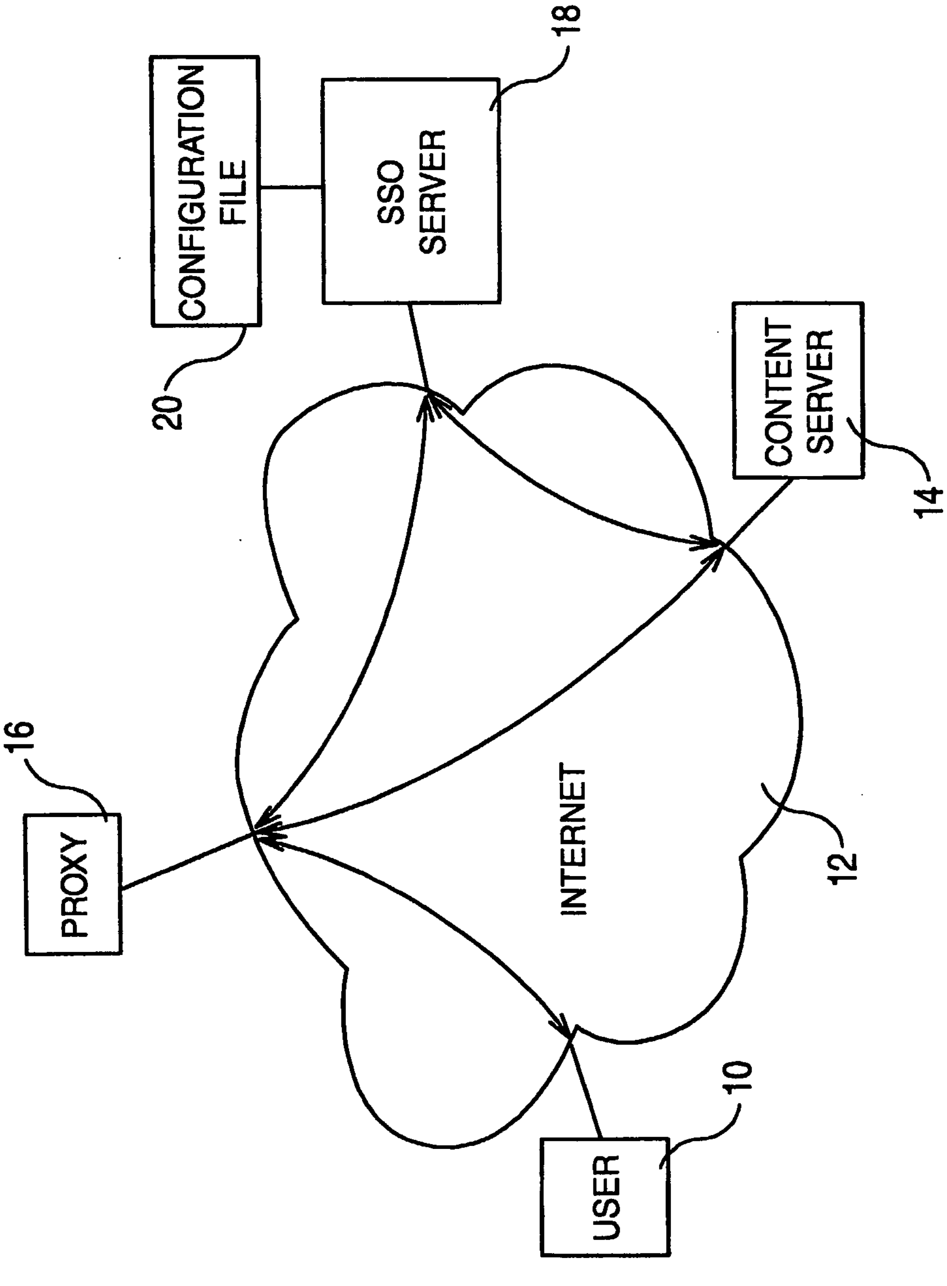
CONFIGURATION FILE
20
SSO SERVER
18
CONTENT SERVER
14
INTERNET
12
PROXY
16
USER
10

FIG. 1

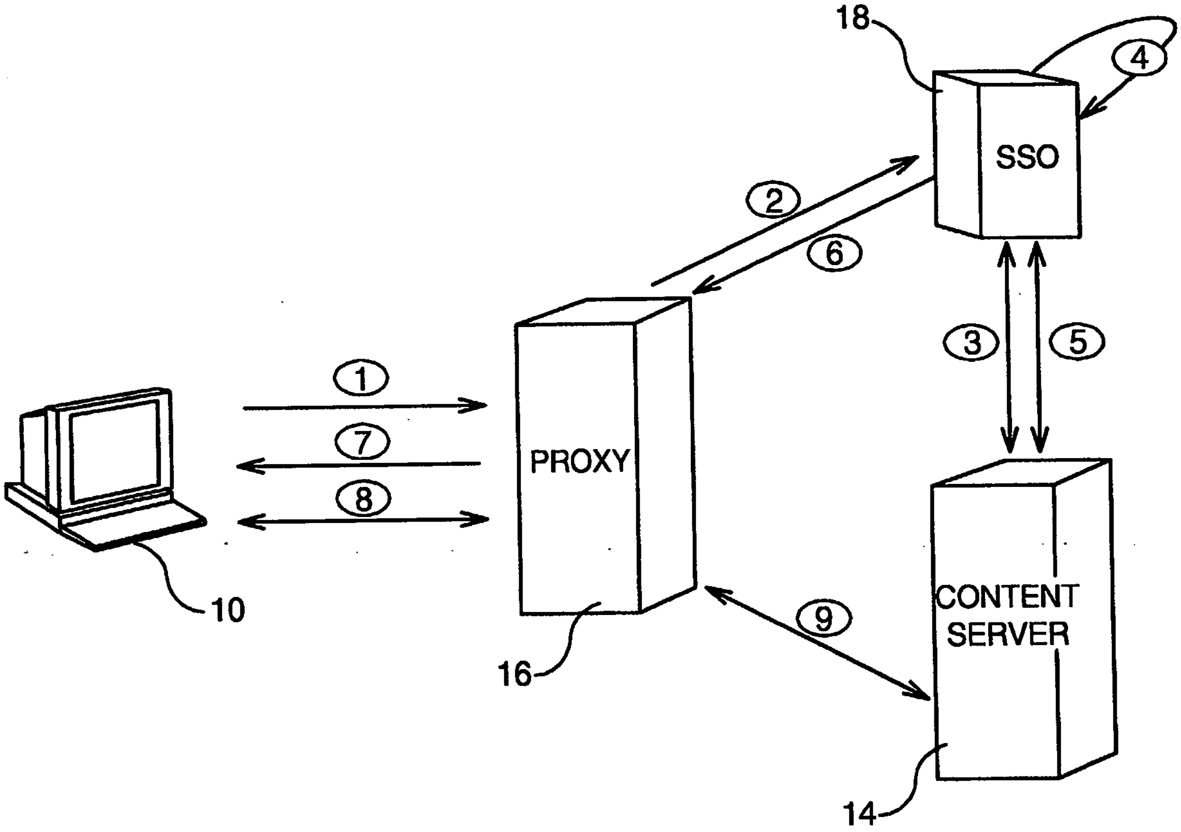

FIG. 2

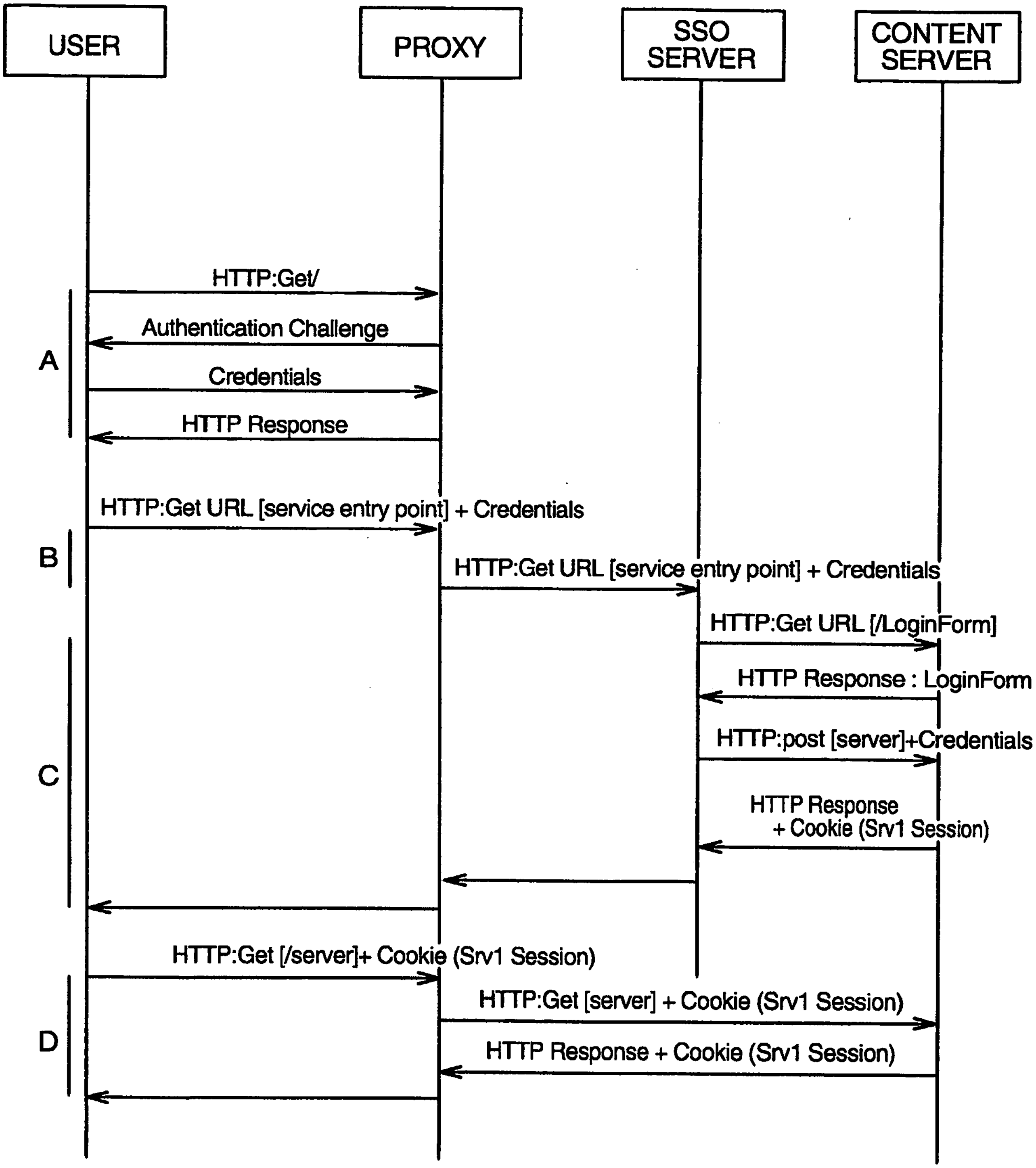
USER
PROXY
SSO SERVER
CONTENT SERVER
HTTP:Get/
Authentication Challenge
A
Credentials
HTTP Response
HTTP:Get URL [service entry point] + Credentials
B
HTTP:Get URL [service entry point] + Credentials
HTTP:Get URL [/LoginForm]
HTTP Response : LoginForm
C
HTTP:post [server]+Credentials
HTTP Response
+ Cookie (Srv1 Session)
HTTP:Get [/server]+ Cookie (Srv1 Session)
D
HTTP:Get [server] + Cookie (Srv1 Session)
HTTP Response + Cookie (Srv1 Session)

FIG. 3